AMENDMENTS TO THE SPECIFICATION

In the Specification:

Please replace the paragraph beginning on page 3, line 8, with the following amended paragraph:

The system design allows the dialog session key to be independently ~~management~~ managed by each endpoint (*e.g.,* service). This makes updating the dialog session key very easy and lightweight compared to other messaging systems, where both endpoints must agree on the updated session key.

Please replace the paragraph beginning on page 8, line 28, with the following amended paragraph:

Because the system 100 gives each endpoint the freedom to generate its own dialog session key, the endpoint has total leeway in deciding when and how often it updates the dialog session key ~~is employs~~ it employs for message(s) it sends. This is not the case in traditional messaging systems, where generally both endpoints need to agree in order to update a shared session key. A drawback of a shared session key is that the key update process can become very expensive as it requires this two-way handshaking. Additionally, two way handshaking can require that the endpoints be directly addressable (*e.g.,* firewalls can prevent this) and have common lifetimes (*e.g.,* they have to be available during the same time).

Please replace the paragraph beginning on page 11, line 7, with the following amended paragraph:

~~System(s) (s)~~ System(s) and method(s) of employing a key exchange key and a dialog session key to facilitate secure communication are set forth in greater detail in co-pending U.S. utility application No. _____ (Attorney docket reference MSFTP624US), filed on April __, 2004 and entitled "SESSION KEY EXCHANGE KEY" which is incorporated herein by reference.

Please replace the paragraph beginning on page 14, line 13, with the following amended paragraph:

The security preamble 310 can include ~~information~~ general security information. In one example, the security preamble 310 includes:

Please replace the paragraph beginning on page 17, line 17, with the following amended paragraph:

For example, when the initiator begins a second dialog can use the service pair header 320 and the key exchange key header 330 that were computed for the first dialog. When the target receives the message, it notices that it already cached the key exchange key 280 and can go ahead and decrypt the "per dialog" dialog session key 290. It can ~~than~~ then use the dialog session key 290 to decrypt the messages sent by the initiator as well as verify its MIC.